(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－159053
（P2002－159053A）
(43)公開日　平成14年５月31日(2002.5.31)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｊ１０４
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｋ０３３
9/32			６０１Ｅ	５Ｋ０６７
12/28			６７５Ｂ	
		11/00	３１０Ｂ	

審査請求　未請求　請求項の数15　ＯＬ　（全 20 頁）

(21)出願番号　特願2000－351066(P2000－351066)

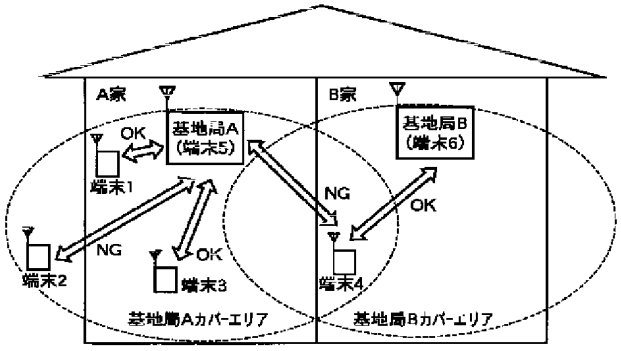
(22)出願日　平成12年11月17日(2000.11.17)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　中北　英明
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　高畠　由彰
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100083806
弁理士　三好　秀和　（外７名）

最終頁に続く

(54)【発明の名称】　無線通信システムで用いられる登録・認証方法

(57)【要約】
【課題】　無線端末同士や、無線基地局と無線端末との間での登録・認証を、確実かつ容易に実行可能な登録・認証方法を提供する。
【解決手段】　無線基地局、無線端末は、それぞれ、通常モード、登録モード、認証モードからなる３つのモードを有しており、どちらも通常モードから登録モード、認証モード、そして再び通常モードと順に移行することで、無線端末の無線基地局に対する登録・認証処理が実行される。無線基地局、無線端末のモード移行の一部について利用者からのマニュアル操作を要求することで、正当ではない利用者による無線端末の登録・認証を抑制する。



【特許請求の範囲】
【請求項１】　無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。
（ａ）利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替える段階；
（ｂ）前記利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替えると共に、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；
（ｃ）前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信し、前記無線基地局のモードを登録モードから認証モードに切り替える段階；
（ｄ）前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；
（ｅ）前記無線端末のモードが認証モードに移行した後、前記無線基地局が前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；
（ｆ）前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；
（ｇ）前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階
【請求項２】　無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。
（ａ）利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替える段階；
（ｂ）前記利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替えると共に、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；
（ｃ）前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；
（ｄ）前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；
（ｅ）前記無線端末のモードが認証モードに移行した後、前記利用者が前記無線基地局を操作することで、前記無線基地局のモードを登録モードから認証モードに切り替えると共に、前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；
（ｆ）前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；
（ｇ）前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階
【請求項３】　前記無線基地局は、前記無線基地局のモードが通常モードから登録モードに切り替わった時点から予め定められた第１の時間経過までに前記無線端末から前記登録申請情報を受信できない場合、あるいは前記無線基地局のモードが登録モードから認証モードに切り替わった時点から予め定められた第２の時間経過までに前記無線端末から前記認証受領情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止し、
前記無線端末は、前記無線端末のモードが通常モードから登録モードに切り替わった時点から予め定められた第３の時間経過までに前記無線基地局から前記登録確認情報を受信できない場合、あるいは前記無線端末のモードが登録モードから認証モードに切り替わった時点から予め定められた第４の時間経過までに前記無線基地局から前記認証通知情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止することを特徴とする請求項１または２に記載の登録・認証方法。
【請求項４】　無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから

成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。
（ａ）利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替える段階；
（ｂ）前記利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替えると共に、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；
（ｃ）前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信し、前記無線基地局のモードを登録モードから認証モードに切り替える段階；
（ｄ）前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；
（ｅ）前記無線端末のモードが認証モードに移行した後、前記利用者が前記無線端末を操作することで、前記無線端末の前記無線基地局に対する認証申請を示す認証申請情報を前記端末秘密鍵および端末暗号方式を用いて暗号化して前記無線基地局に送信する段階；
（ｆ）前記暗号化された認証申請情報を前記無線基地局が前記端末公開鍵を用いて復号できた場合に、前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；
（ｇ）前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；
（ｈ）前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階
【請求項５】　前記無線基地局は、前記無線基地局のモードが通常モードから登録モードに切り替わった時点から予め定められた第１の時間経過までに前記無線端末から前記登録申請情報を受信できない場合、あるいは前記無線基地局のモードが登録モードから認証モードに切り替わった時点から予め定められた第２の時間経過までに前記無線端末から前記認証申請情報および認証受領情報のうちのいずれかを受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止し、前記無線端末は、前記無線端末のモードが通常モードから登録モードに切り替わった時点から予め定められた第３の時間経過までに前記無線基地局から前記登録確認情報を受信できない場合、あるいは前記無線端末のモードが登録モードから認証モードに切り替わった時点から予め定められた第４の時間経過までに前記無線基地局から前記認証通知情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止することを特徴とする請求項４に記載の登録・認証方法。
【請求項６】　無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。
（ａ）利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替える段階；
（ｂ）前記利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替えると共に、前記無線基地局に対する登録受付可能を示す登録受付情報を前記無線端末に送信する段階；
（ｃ）前記無線端末が前記登録受付情報を受信すると、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；
（ｄ）前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信し、前記無線基地局のモードを登録モードから認証モードに切り替える段階；
（ｅ）前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替えると共に、前記無線端末の前記無線基地局に対する認証申請を示す認証申請情報を前記端末秘密鍵および端末暗号方式を用いて暗号化して前記無線基地局に送信する段階；
（ｆ）前記暗号化された認証申請情報を前記無線基地局が前記端末公開鍵を用いて復号できた場合に、前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；
（ｇ）前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；

（ｈ）前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階

【請求項７】　無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。

（ａ）利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替える段階；

（ｂ）前記利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替えると共に、前記無線基地局に対する登録受付可能を示す登録受付情報を前記無線端末に送信する段階；

（ｃ）前記無線端末が前記登録受付情報を受信すると、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；

（ｄ）前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信し、前記無線基地局のモードを登録モードから認証モードに切り替える段階；

（ｅ）前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；

（ｆ）前記無線端末のモードが認証モードに移行した後、前記利用者が前記無線端末を操作することで、前記無線端末の前記無線基地局に対する認証申請を示す認証申請情報を前記端末秘密鍵および端末暗号方式を用いて暗号化して前記無線基地局に送信する段階；

（ｇ）前記暗号化された認証申請情報を前記無線基地局が前記端末公開鍵を用いて復号できた場合に、前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

（ｈ）前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；

（ｉ）前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階

【請求項８】　前記無線基地局は、前記無線基地局のモードが通常モードから登録モードに切り替わった時点から予め定められた第１の時間経過までに前記無線端末から前記登録申請情報を受信できない場合、あるいは前記無線基地局のモードが登録モードから認証モードに切り替わった時点から予め定められた第２の時間経過までに前記無線端末から前記認証申請情報および認証受領情報のうちのいずれかを受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止し、前記無線端末は、前記無線端末のモードが通常モードから登録モードに切り替わった時点から予め定められた第３の時間経過までに前記無線基地局から前記登録受付情報および登録確認情報のうちのいずれかを受信できない場合、あるいは前記無線端末のモードが登録モードから認証モードに切り替わった時点から予め定められた第４の時間経過までに前記無線基地局から前記認証通知情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止することを特徴とする請求項６または７に記載の登録・認証方法。

【請求項９】　無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。

（ａ）利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替える段階；

（ｂ）前記利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替えると共に、前記無線基地局に対する登録受付可能を示す登録受付情報を前記無線端末に送信する段階；

（ｃ）前記無線端末が前記登録受付情報を受信すると、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；

（ｄ）前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

（ｅ）前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；

（ｆ）前記無線端末のモードが認証モードに移行した後、前記利用者が前記無線基地局を操作することで、前記無線基地局のモードを登録モードから認証モードに切り替えると共に、前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

（ｇ）前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；

（ｈ）前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階

【請求項１０】　前記無線基地局は、前記無線基地局のモードが通常モードから登録モードに切り替わった時点から予め定められた第１の時間経過までに前記無線端末から前記登録申請情報を受信できない場合、あるいは前記無線基地局のモードが登録モードから認証モードに切り替わった時点から予め定められた第２の時間経過までに前記無線端末から前記認証受領情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止し、

前記無線端末は、前記無線端末のモードが通常モードから登録モードに切り替わった時点から予め定められた第３の時間経過までに前記無線基地局から前記登録受付情報および登録確認情報のうちのいずれかを受信できない場合、あるいは前記無線端末のモードが登録モードから認証モードに切り替わった時点から予め定められた第４の時間経過までに前記無線基地局から前記認証通知情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止することを特徴とする請求項９に記載の登録・認証方法。

【請求項１１】　前記無線端末は、前記無線基地局に対する登録・認証処理が完了した場合には、前記無線端末が登録済みであることを特定する通常モードに移行することを特徴とする請求項１乃至１０に記載の登録・認証方法。

【請求項１２】　前記無線端末は、通常モード、登録モードおよび認証モードのうちのいずれかを設定する状態設定部と、前記状態設定部によって設定されたモードを利用者に表示する状態表示部と、前記端末公開鍵、端末秘密鍵および端末暗号方式を予め保持する端末情報管理部と、取得した前記基地局鍵および基地局暗号方式を格納するシステム認証情報管理部とを備え、前記状態設定部は、前記利用者からモード移行要求を入力した場合には、該モード移行要求にしたがうことを特徴とする請求項１乃至１１に記載の登録・認証方法。

【請求項１３】　前記無線端末は、更に、前記第３および第４の時間を管理するタイマ設定部を備えることを特徴とする請求項３，５，８または１０に記載の登録・認証方法。

【請求項１４】　前記無線基地局は、通常モード、登録モードおよび認証モードのうちのいずれかを設定する状態設定部と、前記状態設定部によって設定されたモードを利用者に表示する状態表示部と、前記基地局共通鍵および基地局暗号方式を予め保持するシステム認証情報管理部と、取得した前記端末鍵および端末暗号方式を格納する端末認証情報管理部とを備え、前記状態設定部は、前記利用者からモード移行要求を入力した場合には、該モード移行要求にしたがうことを特徴とする請求項１乃至１１に記載の登録・認証方法。

【請求項１５】　前記無線基地局は、更に、前記第１および第２の時間を管理するタイマ設定部を備えることを特徴とする請求項３，５，８または１０に記載の登録・認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、無線ＬＡＮを用いた無線通信システム、この無線通信システムを構成する無線端末、無線基地局、この無線通信システムの登録・認証方法に係り、特に、ＩＥＥＥ８０２．１１等の無線ＬＡＮシステムにおける、無線端末同士や、無線基地局と無線端末との間の、登録・認証技術に関する。

【０００２】

【従来の技術】近年のＬＡＮ(Local Area Network)技術の発達に伴い、オフィス環境のネットワーク化がＰＣ(Personal Computer)間の接続を中心として進行している。このような有線ＬＡＮの普及の一方で、有線ＬＡＮの一部分を無線で置換する無線ＬＡＮ化も進んでいる。たとえば、有線ＬＡＮに無線基地局を接続し、この基地局へ複数の携帯型ＰＣを無線で接続する場合である。この携帯型ＰＣを用いて有線ＬＡＮにイーサネット（登録商標）接続されているデスクトップＰＣのファイルを編集すれば、有線ＬＡＮへ無線アクセスを行っていることになる。また、基地局と携帯型ＰＣの部分を切り出してみると、その部分は無線ＬＡＮを形成している。このような無線ＬＡＮの利点としては、伝送路として電波や赤外線などを利用するので配線敷設が不要な点や、ネットワークの新設やレイアウト変更が容易な点が挙げられる。

【０００３】このような無線ＬＡＮの導入はＩＥＥＥ８０２．１１の標準化によって拍車がかかっている。ＩＥＥＥ８０２．１１では、１９９７年に２．４ＧＨｚ帯の無線ＬＡＮ仕様を、１９９９年に５ＧＨｚ帯の無線ＬＡＮ仕様を、それぞれ完成させている。２．４ＧＨｚ帯の無線ＬＡＮ仕様の伝送速度は、１～２Ｍｂｐｓのものと１１Ｍｂｐｓのものがあり、さらに、２０Ｍｂｐｓを超える仕様が現在検討中である。最近、この２．４ＧＨｚ帯仕様に準拠した製品が、各社から発売されるようになり、基地局や無線ＰＣカードが普及価格帯に入りつつある。一方、５ＧＨｚ帯の無線ＬＡＮ仕様では、２０～３０Ｍｂｐｓの伝送速度を実現可能である。また、５ＧＨｚ帯は２．４ＧＨｚ帯とは異なり、現在は気象レーダに

利用されているだけのほぼ未使用な周波数帯域であり、かつ、より高速な伝送速度が容易に見込めるため、次世代の無線ＬＡＮ仕様と期待されている。

【０００４】また、ここに来て、Ｂｌｕｅｔｏｏｔｈが携帯電話業界や、家電業界、ＰＣ業界を巻き込んで、あらゆる機器に搭載されようとしている。このＢｌｕｅｔｏｏｔｈも２．４ＧＨｚ帯の無線システムであるが、１チップ５ドル程度という低コストと、幅広い業種の約２０００社から賛同を得ていることから、世界的な普及がにわかに見込まれている。

【０００５】以上のような状況から、無線ＬＡＮシステムはオフィス環境だけでなく、一般家庭にも普及が進んでいくものと考えられる。したがって、近い将来、複数の無線ＬＡＮシステムが隣接するとか、同一空間に共存するというような環境が広く築かれると予想される。

【０００６】ところで、ＩＥＥＥ８０２．１１では、無線端末間や、無線基地局と無線端末との間の認証処理が規定されている（ＩＥＥＥ８０２．１１仕様書の第８章）。この規定では、認証処理の対象となる２つのエンティティ（無線端末同士、または、無線基地局と無線端末）が、同一の秘密鍵（共通鍵）を使用して認証し、かつ、秘匿通信する方式が記述されている（ただし、この認証処理はオプション扱いである）。この認証処理には、ＷＥＰ(Wired Equivalent Privacy)と呼ばれるアルゴリズムが用いられる。秘密鍵の配布はあらかじめセキュアな方法で行われる、とだけ記載されている。また、秘密鍵は２つのエンティティそれぞれに対応するので、或る無線端末から見れば、システム内の他の無線端末ごとに秘密鍵を有する必要があり、システム全体では無線端末数の二乗オーダーの秘密鍵が必要とされる。

【０００７】ここで、ＷＥＰアルゴリズムによる暗号化と復号化に簡単に触れる。そして、このＷＥＰアルゴリズムを用いた認証についても記述する。図３１は、ＩＥＥＥ８０２．１１のＷＥＰアルゴリズムの暗号化処理の説明図である。図３１では、送信されるデータが暗号化される処理が示されており、特に、その送信されるデータをここでは平文ＰＴと呼ぶ。

【０００８】まず、送信側において、このＰＴからＣＲＣが生成される。すなわち、ＩＣＶが生成される。一方、秘密鍵Ｓｋと初期ベクトルＩＶとから、ＷＥＰ乱数発生器を経て、キーシーケンスＫＳが生成される。このＫＳは、ＰＴとＩＣＶとの連結結果｛ＰＴ，ＩＣＶ｝と長さを合わせた上で、排他的和算される。この排他的和算の結果が暗号文ＥＴである。そして、このＥＴとＩＶに制御コードを合わせることで、図３２に示すＷＥＰフレームを構成する。このＷＥＰフレームによって、ＷＥＰアルゴリズムによる秘匿通信が行われる。

【０００９】図３３に、ＩＥＥＥ８０２．１１のＷＥＰアルゴリズムの復号化処理の内容を示す。図３３では、受信された暗号化データを復号化する処理が示されている。図３３において、受信側がＷＥＰフレームを受信すると、そのＷＥＰフレームからＩＶを取り出し、秘密鍵Ｓｋと共にＷＥＰ乱数発生器に入力し、キーシーケンスＫＳを発生させる。このキーシーケンスＫＳは、ＩＶが改竄されていなければ、図３１のＫＳと同じものが生成されるはずである。このＫＳをフレーム内の暗号文ＥＴと排他的和算すれば、平文ＰＴとＩＣＶが復号される。このＰＴをＣＲＣチェックし、その結果であるＩＣＶ’と復号されたＩＣＶとを比較することで、ＰＴの正しさを確認する。ＩＣＶ’とＩＣＶが等しければ、ＰＴの受信に成功したことになる。

【００１０】図３４に、ＩＥＥＥ８０２．１１のＷＥＰアルゴリズムによる認証処理のシーケンスチャートを示す。図３４は、無線基地局（基地局）とこの基地局の無線ゾーン内の無線端末（端末）との間で無線通信する例を示している。図３４において、共通鍵である秘密鍵Ｓｋは、基地局と端末との間であらかじめ互いに交換されている（ステップＳ１００１）。そして、まず最初に、端末が基地局へ無線通信で認証要求のフレームを送る（ステップＳ１００２）。この認証要求フレームには、共通鍵方式による認証を要求していることが記入される。なお、上記のステップＳ１００１で、秘密鍵Ｓｋは、基地局および端末の双方へ配布済みである。

【００１１】次に、基地局は、認証要求受理のステータスにあれば、この秘密鍵Ｓｋと内部で発生させた初期ベクトルＩＶから、ＷＥＰ乱数発生器を経て、試験文ＣＴを作成する（ステップＳ１００３）。通常、このＣＴの長さは１２８バイトである。基地局は、作成したＣＴを端末へ無線通信する（ステップＳ１００４）。

【００１２】端末は、基地局から受け取ったＣＴを平文として扱い、上記の図３１に示した方法により秘密鍵Ｓｋで暗号化する（Ｓｋ（ＣＴ））（ステップＳ１００５）。そして、このＳｋ（ＣＴ）を含む暗号文を、端末が基地局へ無線通信する（ステップＳ１００６）。

【００１３】最後に、端末から送られて来た暗号文が基地局で検証され（ステップＳ１００７）、正しければ、端末に向けて、成功ステータスの認証完了フレームが送られる。一方、正しくなければ、失敗ステータスのフレームが送られる（ステップＳ１００８）。この検証は、上記の図３３で示した方法でＳｋ（ＣＴ）を復号した結果であるＳｋ（Ｓｋ（ＣＴ））（＝ＣＴ’）と基地局が最初に作成したＣＴとが同一であるか否かを調べることによって実行される。

【００１４】

【発明が解決しようとする課題】上述したように、無線ＬＡＮシステムの普及に伴って、一般の家庭内で、複数の無線ＬＡＮシステムが隣接したり、同一空間に共存したりする場合が起こり得る。ここで、図１に例示する、集合住宅内の隣接した２軒の家、Ａ家およびＢ家それぞれに家庭内無線通信システムが設置されている場合を考

えてみる。

【００１５】図１の例では、Ａ家に無線基地局Ａが、Ｂ家に無線基地局Ｂがそれぞれ設置されている。しかしながら、基地局Ａ，Ｂのカバーエリアは、それぞれの基地局Ａ，Ｂが設置された家Ａ，Ｂからはみ出してしまう可能性が十分にある。たとえば、Ａ家の基地局Ａから見れば、Ａ家に属する端末１，３のみならず、屋外の端末２や、Ｂ家の端末４も、基地局Ａのカバーエリア内に存在してしまっている。しかしながら、屋外の端末２、Ｂ家の端末４は、Ａ家に属する端末ではないので、基地局Ａは端末２，４から登録・認証要求があっても、端末２，４には認証を与える必要はない。すなわち、基地局Ａが認証すべき端末は、Ａ家の端末である端末１，３だけである。したがって、基地局Ａは、Ａ家の端末１，３以外に認証を与えないように、端末の登録・認証を管理するようにしたい。Ｂ家の基地局Ｂにおいても、同様のことが言える。

【００１６】さらに、家庭内の機器には、異なる製造メーカ間であっても、機器同士の相互接続性が要求される。メーカ独自仕様が許容されるＩＥＥＥ８０２．１１のような無線ＬＡＮでは、秘密鍵の配布は、図３４のステップＳ１００１で行えば良い。たとえば、あらかじめ秘密鍵を基地局や端末に作り込んでおけば良い。しかしながら、家庭内無線通信システムでは、無線によるセキュアかつ容易な方法で、異なるメーカの装置間で秘密鍵を交換できる仕組みが別途必要となる。

【００１７】本発明は、かかる事情に鑑みて成されたものであり、その目的は、ＩＥＥＥ８０２．１１等の無線通信システムであって、無線端末同士や、無線基地局と無線端末との間での登録・認証を、確実かつ容易に実行可能な無線通信システムを提供することである。

【００１８】

【課題を解決するための手段】ここで開示される発明のうち代表的なものの概要を説明すれば次の通りである。すなわち、無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、（ａ）利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替える段階；（ｂ）前記利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替えると共に、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；（ｃ）前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信し、前記無線基地局のモードを登録モードから認証モードに切り替える段階；（ｄ）前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；（ｅ）前記無線端末のモードが認証モードに移行した後、前記無線基地局が前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；（ｆ）前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；（ｇ）前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階、を含む登録・認証方法であることである。

【００１９】本発明に係る登録・認証方法では、たとえば家庭内に設置された無線基地局に対して無線端末の登録・認証を行う場合、無線端末の利用者は無線基地局を直接操作しなければならない。このため、無線基地局の操作が容易でない外部の利用者の無線端末の登録・認証を防止できる。それにより、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実現できる。

【００２０】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態を詳細に説明する。本発明の主な対象は、家庭内無線通信システムである。このシステムでは、管理上は無線基地局が無線端末の登録および認証を行い、通常のデータ通信が端末間で直接行われる。端末は、公開鍵暗号方式による暗号方式と、その秘密鍵および公開鍵を持つことが前提である。公開鍵暗号方式としては、たとえば、ＲＳＡ暗号方式や楕円暗号方式が挙げられる。基地局は、共通鍵暗号方式による暗号方式と、その共通鍵を持つことが前提である。共通鍵暗号方式としては、たとえば、ＤＥＳ方式やＡＥＳ方式などが挙げられる。

【００２１】本発明では、まず、端末の公開鍵暗号方式で登録を行い、次に、基地局の共通鍵暗号方式で認証を行う。したがって、本発明は、通常のデータと同じ無線通信方式を用いて、基地局が端末を登録および認証し、その結果、認証を受けた端末同士は、基地局管理の共通鍵方式でシステム内秘匿通信をすることができる。本発明によって、認証を受けていない外部端末が、システム内の通信を傍受することや、システム内の端末としてなりすましを防止できる。また、本発明は、ＩＥＥＥ８０２．１１のＷＥＰアルゴリズムにおいて前提となっているデータ通信用秘密鍵の事前配布方法として使用するこ

とも可能である。この場合には、本発明方式の利用後、ＷＥＰアルゴリズムで、ＩＥＥＥ８０２．１１としての端末認証を行うことになる。

【００２２】基地局は、家庭内無線通信システムの管理上の責任を負うだけで、それ以外の機能は他の端末と何ら変わらない。逆に言うと、端末の登録・認証機能を基地局機能と呼ぶことにすると、この基地局機能をもつ端末が基地局になることも可能であり、この考え方はＩＥＥＥ１３９４にも通ずるものである。このため、たとえば、図１に示すように、基地局Ａを「端末（端末５）」、基地局Ｂを「端末（端末６）」として扱うこともできる。

【００２３】以下、本発明の実施の形態に係る無線通信システムについて６つの実施例を用いて説明する。第１乃至第６の実施例は、それぞれ、図１の基地局Ａに端末１を登録および認証する場合を示している。本発明の特徴は、利用者が、端末および基地局の両方を操作しながらそれぞれの状態を確認しつつ、端末の登録・認証を進めていく点にある。このため、無線通信によりながらも、セキュアかつ容易に、端末の登録・認証を実現できる。すなわち、端末や基地局の操作を利用者に要求することで、利用者はボタンを押す順序などのシーケンスに正しく従う必要がある。また、外部から家屋内の基地局Ａをマニュアル操作することは困難である。このため、たとえば、図１の端末２や端末４が基地局Ａに登録することは基本的に不可能である。万が一、これら外部の端末２，４を、Ａ家の端末１あるいは端末３の登録・認証のときに、横槍を入れて登録・認証させようとしても、基地局Ａや端末１あるいは端末３の状態表示で、そのような動作をＡ家の利用者は簡単に検出することができる。

【００２４】（第１の実施例）次に、図２および図３を用いて、本発明の実施の形態に係る無線通信システムの第１の実施例を説明する。図２は、この第１の実施例に係る無線通信システムの登録・認証シーケンスチャートである。ここでは、図１の基地局Ａ（端末５）と端末１との間での登録・認証シーケンス（登録・認証シーケンス１）が示されている。この登録・認証シーケンス１は、大きく分けて、登録段階と認証段階とに分けられる。なお、図２では、時刻ｔは上から下に経過していくものとする。これらは、後述の他の実施例のシーケンスにおいても同様である。図３は、基地局Ａと端末１との間で交換される情報に焦点をあてて、図２の登録・認証シーケンス１を説明するものである。図３に示された丸囲み数字は、登録・認証シーケンス１の進行順を示している。この登録・認証シーケンス１では、端末１から基地局Ａへ登録申請情報および認証受領情報が無線通信される。また、基地局Ａから端末１へ登録確認情報および認証通知情報が無線通信される。以下、図２を参照して、この登録・認証シーケンス１を説明する。

【００２５】基地局Ａは、①通常モード、②登録モード、および、③認証モードを有している。また、端末１も、①２種類の通常モード、すなわち、未登録通常モードと登録済み通常モード、②登録モード、および、③認証モードを有している。もちろん、基地局Ａと同様、通常モードは１種類であっても構わない。通常モードが２種類の場合、端末１の登録は１回だけに限定され、結果として、１基の基地局だけに登録可能となる。一方、通常モードが１種類の場合には、複数の基地局に登録することができる。端末１の登録が１回に限定されないからである。なお、図２では、基地局Ａおよび端末１のＬＥＤ表示について次の表記を用いる。「Ｒ」は赤色点灯で、登録モードを表す。「Ｇ」は緑色点灯で、登録済み通常モードを表す。「＜Ｒ＞」は赤色点滅で、認証モードを表す。「＜Ｇ＞」は緑色点滅で、未登録通常モードを表す。なお、ＬＥＤ表示の例は、他にもバリエーションが考えられる。たとえば、認証モードは黄色点灯などである。また、図２の基地局Ａ、端末１の直角三角形表示は、利用者によるボタン操作を表している。

【００２６】（ａ）まず、利用者は、基地局Ａの登録ボタンの操作によって、基地局Ａのモードを通常モードから登録モードに切り替える（時刻ａ、ステップＳ１０１）。また、この時、タイマ１がスタートする。

【００２７】（ｂ）次に、利用者は、端末１の登録ボタンを押す（時刻ｂ、ステップＳ１０２）。その操作に応じて、端末１は基地局Ａに登録申請情報を無線送信する（ステップＳ１０３）。また、端末１の登録ボタンが押された時点で、タイマ３がスタートする。この登録申請情報の送信の後、端末１のモードも通常モードから登録モードに切り替わる。この時点で、基地局Ａと端末１の両方が登録モードに移行したことになる。

【００２８】端末１が送信する登録申請情報には、図４に示すように、端末１のＭＡＣアドレス、端末１の公開鍵および公開鍵暗号方式、その他端末１固有の情報（機器種別、シリアル番号、製造会社名、利用者氏名等）が含まれる。ＭＡＣアドレスとしては、ＩＥＥＥのＥＵＩ６４アドレスまたはＥＵＩ４８アドレスが考えられる。これらのアドレスによれば、端末１を一意に特定できるからである。ＥＵＩ６４アドレスは、前半の２４ビットと後半の４０ビットに分けられ、前半部分がＩＥＥＥによって割り当てられるＣｏｍｐａｎｙＩＤで、後半部分はこのＣｏｍｐａｎｙＩＤが割り当てられた会社が自由に使用することができる。たとえば、ＡＣ－ＤＥ－６４－００－００－００－００－８０（ヘキサ表示）というアドレスが示される。ＩＥＥＥ１３９４ではノード（端末）固有のアドレスとしてＥＵＩ６４を用いる。ＥＵＩ４８アドレスはイーサネットアドレスなどで使用されており、後半部分が２４ビットである点を除けば、ＥＵＩ６４とほぼ同じである。また、ＥＵＩ６４アドレスで、後半部分の最初の２オクテットをＦＦ－ＦＥ（ヘキサ表

示）に設定すれば、ＥＵＩ４８アドレスフォーマットとして使用することができる。

【００２９】公開鍵および公開鍵暗号方式は、端末１があらかじめ保有しているものである。これらは、たとえば、製品出荷時に端末１自身に搭載されたＲＯＭなどに書き込まれたり、端末１の無線インタフェースカードのＲＯＭに書き込まれたりする。

【００３０】端末１固有情報の例としては、機器の種別やシリアル番号や製造会社名、利用者の氏名などの情報が考えられる。これらの情報はコード化して管理してもよい。たとえば、機器種別を４ビットで表現して、００００がワイヤレスＴＶ、０００１がデジタルＶＣＲ、００１０がノートＰＣなどと決めておけば良い。製造会社名も、００００００が東芝、０００００１がソニーなどとあらかじめ割り当てておけば良い。

【００３１】（ｃ）基地局Ａは、端末１からの登録申請情報を受理した場合、端末１へ登録確認情報を返す（時刻ｃ、ステップＳ１０４）。この登録確認情報は、基地局Ａ側で端末１を登録することができたことを端末１側に報告するものである。この時、基地局Ａのモードが登録モードから認証モードに切り替わる。また、タイマ２もスタートする。登録確認情報は、登録申請情報によって端末１から受理した端末１の公開鍵により暗号化されている。この暗号化によって、登録申請を要求した端末１だけが登録確認情報の中身を読むことができる。この登録確認情報には、図５に示すように、登録がＯＫであることを示すフラグ、登録ＯＫの対象である端末１のＭＡＣアドレス、端末固有情報などが含まれる。これらの端末ＭＡＣアドレスや端末固有情報などは、上記の図４の登録申請情報から得られるものである。

【００３２】（ｄ）基地局Ａからの登録確認情報の受理によって、端末１のモードが、登録モードから認証モードに切り替わる（時刻ｄ）。この時、タイマ４がスタートする。

【００３３】（ｅ）認証モードへの移行時点（時刻ｃ）からあらかじめ定められた時間経過後、基地局Ａは認証通知情報を端末１へ送信する（時刻ｅ、ステップＳ１０５）。この時刻ｅと時刻ｄとの関係は、端末１が確実に認証モードにある時に認証通知を受信できるように配慮される。認証通知情報には、図６に示すように、認証通知、基地局ＡのＭＡＣアドレス、基地局Ａの共通鍵と共通鍵暗号方式、そして、基地局Ａの固有情報が含まれる。そして、登録確認情報と同様に、端末１の公開鍵および公開鍵暗号方式を用いて暗号化されている。端末１だけが公開鍵と対の秘密鍵を持っているので、それ以外の端末は端末１への認証通知情報を確認することができない。

【００３４】（ｆ）端末１が認証通知情報を受理すると、認証受領情報を基地局Ａへ返信する（時刻ｆ、ステップＳ１０６）。この時、端末１のモードは、認証モードから通常モード（緑色点灯表示）に切り替わる。登録および認証処理の当初、未登録通常モード（緑色点滅）だった端末１は、登録済み通常モード（緑色点灯）となる。一方、当初は通常モード（緑色点灯表示）だった基地局Ａは、元に戻る。認証受領情報は、図７に示すように、端末１が認証通知を受領したこと（認証ＯＫ）を、端末１の端末アドレスや基地局ＭＡＣアドレスとともに含むものである。これらは、基地局Ａの共通鍵および共通鍵暗号方式で暗号化され、基地局Ａへ送信される。

【００３５】（ｇ）基地局Ａは、端末１からの認証受領情報を正しく復号できた場合に、認証モードから通常モードに戻る（時刻ｇ）。この時、時刻ｇで端末１も基地局Ａも通常モードになっている場合、この端末１は基地局Ａに登録・認証され、処理が完了する。

【００３６】このようにして登録・認証された端末１は、基地局Ａが管理する家庭内無線通信システムの中で、基地局Ａの共通鍵暗号方式を利用することが可能となり、他の認証済み端末と秘匿通信できるようになる。たとえば、図８に示すように、端末間通信データが秘匿される。すなわち、図８は、基地局Ａが家庭内無線通信システム管理している例で、基地局Ａがあらかじめ保持する共通鍵ＳＫｓａおよびその暗号化方式ＳＡｓａを用いて暗号化している。この場合、基地局Ａから登録・認証を受けない限り、この秘匿通信データを各端末は読むことができない。

【００３７】図９は、基地局Ａによって管理される登録認証テーブルの内容を示す図である。この登録認証テーブルには、端末ごとに、ＭＡＣアドレス、公開鍵、暗号方式、端末固有情報などが記録されている。これらの端末ごとのデータは、上記の図４に例示した、各端末の登録申請情報から得られる。もちろん、このテーブルには基地局Ａ自身の情報も含まれる。基地局Ａ自身の情報としては、基地局Ａがあらかじめ保持する共通鍵およびその共通鍵暗号方式が挙げられる。さらに、基地局Ａが端末として機能する際に必要な情報である、ＭＡＣアドレス、公開鍵暗号方式による公開鍵、秘密鍵およびその暗号方式、他の端末固有情報も含まれる。

【００３８】上記の第１の実施例では、図２のタイマ（タイマ１～タイマ４）を用いて、登録・認証の失敗をハンドリングし、基地局Ａや端末１を通常モードに戻すことが可能である。以下、この際のタイマの動作について、図１０乃至図１４を用いて説明する。

【００３９】（１）図１０は、端末１が登録申請情報を基地局Ａへ送信したが、基地局Ａがこの情報をうまく受信できず、その結果、登録確認情報を返信できなかった場合のシーケンスチャートである。この場合、基地局Ａでは、時刻ａでタイマ１がスタートしたが、時刻ｃで時間切れになり、元の通常モードに戻る。一方の端末１も、時刻ｂでタイマ３がスタートしたが、登録申請情報の返事、すなわち、登録確認情報をもらえないまま、時

刻ｄに時間切れとなり、元の通常モードに戻る。基地局Ａも端末１も、認証モードに入らずに通常モードに戻るので、失敗したことは視覚的に判断できる。また、タイマ１とタイマ３の制限時間を登録・認証に要する時間よりも長めに設定しておけば、その時間の長さも視覚的判断材料とすることができる。

【００４０】（２）図１１は、端末１が基地局Ａからの登録確認情報を正しく復号できなかった場合のシーケンスチャートである。この場合、端末１は登録確認情報を正しく受け取ることができないため、タイマ３が時間切れとなり、端末１のモードは元の通常モードに戻ってしまう。その結果、基地局Ａは、端末１から認証受領情報を受け取ることができないので、同様にタイマ２が時間切れとなり、基地局Ａのモードも元の通常モードに戻ることになる。

【００４１】なお、基地局Ａのタイマ１は登録確認情報を端末へ送出した時刻ｃに正常に解除される。

【００４２】（３）図１２は、端末１が基地局Ａからの認証通知情報を正しく受け取れなかった場合のシーケンスチャートである。すなわち、上記の図２に示したように、通常、タイマ２のスタート時刻ｃから一定時刻経過後、基地局Ａは認証通知情報を端末１へ送信することになっている。しかしながら、この認証通知情報の端末１への送信が何らかの理由で失敗する場合が想定される。この場合、基地局Ａは、認証通知情報の受信失敗の結果として、端末１から認証受領情報を受け取ることはできない。このため、タイマ２は時間切れとなり、基地局Ａのモードは元の通常モードに戻ることになる。一方、端末１は、基地局Ａから認証通知情報を受信できず、タイマ４が時間切れとなって、元の通常モードに戻る。

【００４３】なお、基地局Ａのタイマ１は、登録確認情報を端末１へ送出した時刻ｃで、正常に解除されている。また、端末１のタイマ３も、登録確認情報を正しく復号できた時刻ｄで、正常に解除されている。

【００４４】（４）図１３は、端末１が基地局Ａからの認証通知情報を正しく復号できなかった場合のシーケンスチャートである。この場合、端末１は、上記の（３）の場合と同様、基地局Ａから認証通知情報を正しく受け取ることができない。このため、タイマ４が時間切れとなって、端末１は元の通常モードに戻る。一方、基地局Ａも、上記の（３）と同様、端末１から認証受領情報を受信できず、タイマ２が時間切れとなり、元の通常モードに戻る。

【００４５】なお、基地局Ａのタイマ１は、登録確認情報を端末１へ送出した時刻ｃで、正常に解除されている。また、端末１のタイマ３も、登録確認情報を正しく復号できた時刻ｄで、正常に解除されている。

【００４６】（５）図１４は、基地局Ａが端末１からの認証受領情報を正しく復号できなかった場合のシーケンスチャートである。この場合、基地局Ａは、端末１からの認証受領情報を復号できないので、タイマ２が時間切れとなり、元の通常モードに戻る。一方、端末１は、基地局Ａからの認証通知情報を正しく受信できたので、正常な動作として、元の通常モードに戻る。また、基地局Ａの認証受領情報の復号失敗は、タイマ２の時間切れによって検出されることになる。このタイマ２の制限時間を正常終了時よりも長く設定した場合には、基地局Ａの認証モードに滞在する時間の増大によって、認証受領情報の復号か失敗を判断できる。

【００４７】なお、基地局Ａのタイマ１は、登録確認情報を端末１へ送出した時刻ｃで、正常に解除されている。また、端末１のタイマ３も、登録確認情報を正しく復号できた時刻ｄで、正常に解除されている。さらに、端末１のタイマ４も認証受領情報を基地局Ａへ送出した時刻ｆで、正常に解除されている。

【００４８】上記の（１）乃至（４）において、端末１の通常モードが未登録通常モードと登録済み通常モードに分かれている場合は、登録・認証に失敗した時、端末１が未登録通常モードに戻ることになる。この場合には、通常モードが１つの場合と比べて、利用者がより視覚的に判断することが可能となる。

【００４９】上記の第１の実施例では、１つの登録・認証シーケンスによっては１つの端末しか登録・認証を受けることができない。以下、この点について、図１５を用いて説明する。図１５の例では、端末２の方が端末１よりも早く登録ボタンを押したため（ステップＳ１０２、ステップＳ１０２’）、端末２の登録申請情報が受理され（ステップＳ１０３、ステップＳ１０３’）、その結果として登録・認証を受けることができた。一方の端末１は、登録ボタンを押した時点ｔｓから、登録モードであったが、時刻ｔｅでタイマ１が時間切れとなり通常モードに戻っている。このタイマ１の時間切れと、認証モードに入らなかったこととから、端末１の登録・認証失敗が判断できる。このように、基地局が、登録申請情報を登録モード期間中だけ受け付け、かつ、１つの端末からの登録・認証要求だけしか受け付けないことにすると、端末の登録・認証は、同時には１つの端末だけであることが保証されることになる。これによれば、他家もしくは外部の端末を誤って登録・認証したことも推定できるので、端末の登録・認証をやり直すことができる。たとえば、図１５の端末１が内部端末、端末２が外部端末であるとする。この場合、内部端末１が失敗したにも関わらず、基地局が正しいシーケンスを辿っていることが一目瞭然なので、何らかの端末（ここでは、外部端末２）が誤って登録・認証された可能性があると判断できる。このように判断できることにより、内部端末１の登録・認証をやり直したり、基地局の登録認証テーブル（図９参照）を修正したりすることが可能である。基地局の登録認証テーブルの修正は、最新情報のみの削除や全情報の削除などが行える。

【００５０】また、上記の第１の実施例において、図２の登録確認情報の送信（ステップＳ１０４）と認証通知情報の送信（ステップＳ１０５）とを兼ねてしまうシーケンスも考えられる。この場合には、基地局Ａは、端末１からの登録申請情報を受理した時、図５の登録確認情報と図６の認証通知情報とを結合し、端末１の公開鍵暗号方式の公開鍵と暗号化アルゴリズムとにより暗号化した後、返信することになる。この登録確認・認証通知を受理した時に、端末１のモードは認証モードに移行する。この認証モードの最中に認証受領情報を作成する。そして、認証受領情報を基地局Ａへ送信したとき、端末１は通常モードに切り替わる。

【００５１】以上説明したように、上記の第１の実施例によれば、基地局Ａの登録ボタンを操作してから、基地局Ａのタイマ１がタイムアウトする前に、端末１の登録ボタンを操作する必要がある。このため、家屋内にある基地局Ａを外部から操作することが困難なことと合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【００５２】（第２の実施例）次に、図１６および図１７を用いて、本発明の実施の形態に係る無線通信システムの第２の実施例を説明する。図１６は、この第２の実施例に係る無線通信システムの登録・認証シーケンスチャートである。図１６の登録・認証シーケンス（登録・認証シーケンス２）が上記の第１の実施例の登録・認証シーケンス１と異なる点は、時刻ｅで基地局Ａが認証通知情報を送る際（ステップＳ２０６）、明示的に認証ボタンを押す点である（ステップＳ２０５）。この認証ボタンは、登録ボタンと別々に配置しても良いし、同一ボタンであっても良い。同一のボタンで構成する場合には、短く（たとえば１秒以内）押したとき登録ボタンで、長く（たとえば数秒）押したとき認証ボタンとしてもよい。このほかにも様々なバリエーションが考えられる。いずれにせよ、このように認証ボタンを利用すると、端末が登録モードから認証モードに変わったことを利用者が確認した後に、明示的に認証ボタンで認証動作をスタートさせることができる。したがって、上記の第１の実施例の登録・認証シーケンス１よりも、登録段階が終了して認証段階に入ったことを、利用者が容易に認識できる。

【００５３】図１６のタイマ（タイマ１、タイマ２、タイマ３、タイマ４）は、タイマ２のスタートが異なる点を除いて、図２の登録・認証シーケンス１と同様である。また、タイマの用途も、シーケンス１と同様で、図１０乃至図１４と同様に動作する。図１６の基地局Ａのタイマ２は、基地局Ａの認証ボタンを利用者が押した時点からスタートする。認証受領情報を正しく復号できた時に解除され、それ以外の異常時には制限時間を超えたところで解除される。

【００５４】図１７は、基地局Ａと端末１との間で交換される情報に焦点をあてて、図１６の登録・認証シーケンス２を説明するものである。図１７の丸囲み数字は登録・認証シーケンス２の進行順を示すものである。この登録・認証シーケンス２では、端末１から基地局Ａへ登録申請情報および認証受領情報が無線通信される。一方、基地局Ａから端末１へ登録確認情報および認証通知情報が無線通信される。

【００５５】この第２の実施例は、上記の第１の実施例と比べて、認証通知と端末の認証モードへの切り替わりとの相関が明確なため、所望でない端末の誤った登録・認証を防止できる点が有利である。第１の実施例で述べた図１１、図１３、図１４の例では、端末１の登録・認証の失敗は、別の端末が誤って登録・認証されたことが原因である可能性もある。これは、基地局Ａからの認証通知の返信タイミングを端末１が把握できないためである。これに対し、この第２の実施例では、端末１が認証モードになったことを確認してから、利用者が基地局Ａの認証ボタンを操作するため、この返信タイミングは明確である。したがって、基地局Ａが別の端末を誤って登録・認証してしまうことを防止できる。

【００５６】以上説明したように、この第２の実施例によれば、基地局Ａの登録ボタンを操作してから、基地局Ａのタイマ１がタイムアウトする前に、端末１の登録ボタンを操作する必要があり、また、端末１が認証モードに切り替わった後、基地局Ａの認証ボタンを操作する必要がある。このため、家屋内にある基地局Ａを外部から操作することが困難なことと合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【００５７】（第３の実施例）次に、図１８および図１９を用いて、本発明の実施の形態に係る無線通信システムの第３の実施例を説明する。図１８は、この第３の実施例に係る無線通信システムの登録・認証シーケンスチャートである。図１８の登録・認証シーケンス（登録・認証シーケンス３）が上記の第２の実施例の登録・認証シーケンス２と異なる点は、基地局Ａの認証ボタンではなく、端末１の認証ボタンを、利用者が明示的に押す点である（ステップＳ３０５）。このようにすると、端末１が登録モードから認証モードに変わったことを利用者が確認してから、端末１の方で、認証ボタンで認証申請し（ステップＳ３０６）、その結果として、認証通知を経て（ステップＳ３０７）、認証受領という動作になる（ステップＳ３０８）。上記の登録・認証シーケンス１，２とは異なり、この登録・認証シーケンス３では、利用者による端末１の認証ボタンの操作が実行される（ステップＳ３０５）。ステップＳ３０６の認証申請情報は、図２０に示すように、認証申請要求、端末１のＭＡＣアドレス、そして、端末固有情報を含んでいる。これらのデータは、端末１の公開鍵方式の秘密鍵を用いて暗号化され、端末１から基地局Ａへ送信される。ここで

注目すべきは、端末１の秘密鍵が使用されていることである。したがって、この鍵と対を成している公開鍵を利用しないと復号できない。これは、端末１によるデジタル署名である。このデジタル署名によって、時刻ｄまでに登録完了済みの端末１が送出した認証申請情報かどうかを判定することができる。

【００５８】図１９は、基地局Ａと端末１との間で交換される情報に焦点をあてて、図１８の登録・認証シーケンス３を説明するものである。図１９の丸囲み数字は登録・シーケンスの進行順を示すものである。この登録・認証シーケンス３では、端末１から基地局Ａへ登録申請情報、認証申請情報および認証受領情報が無線通信される。また、基地局Ａから端末１へ登録確認情報および認証通知情報が無線通信される。

【００５９】この第３の実施例は、上記の第２の実施例と同様、認証通知と端末の認証モードへの切り替わりとの相関が明確なため、所望でない端末の誤った登録・認証を防止できる。

【００６０】以上説明したように、この第３の実施例によれば、基地局Ａの登録ボタンを操作してから、基地局Ａのタイマ１がタイムアウトする前に、端末１の登録ボタンを操作する必要があり、また、端末１が認証モードに切り替わった後、基地局Ａのタイマ２がタイムアウトする前に、端末１の認証ボタンを操作する必要がある。このため、家屋内にある基地局Ａを外部から操作することが困難なことと合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【００６１】（第４の実施例）次に、図２１および図２２を用いて、本発明の実施の形態に係る無線通信システムの第４の実施例を説明する。図２１は、この第４の実施例に係る無線通信システムの登録・認証シーケンスチャートである。図２２は、基地局Ａと端末１との間で交換される情報に焦点をあてて、図２１の登録・認証シーケンス（登録・認証シーケンス４）を説明するものである。図２２に示された丸囲み数字は、登録・認証シーケンス４の進行順を示している。この登録・認証シーケンス４では、端末１から基地局Ａへ登録申請情報、認証申請情報および認証受領情報が無線通信される。また、基地局Ａから端末１へ登録受付情報、登録確認情報および認証通知情報が無線通信される。以下、図２１を参照して、この登録・認証シーケンス４を説明する。

【００６２】（ａ）まず、利用者は、端末１の登録ボタンを押す（時刻ａ、ステップＳ４０１）。つまり、端末１の方から先に登録モード（ＬＥＤ表示は赤色点灯）に移行する。この時、タイマ３がスタートする。

【００６３】（ｂ）次に、利用者は、基地局Ａの登録ボタンを押す（時刻ｂ、ステップＳ４０２）。登録ボタンが押されると、基地局Ａは、図２３に示す登録受付情報を、端末１へ送信する（ステップＳ４０３）。この時、基地局Ａは、登録モードに移行し、そのＬＥＤ表示は赤色点灯となる。また、同時に、タイマ１もスタートする。図２３に示すように、登録受付情報には、登録受付可能を示すフラグ、および、基地局ＭＡＣアドレスが含まれる。

【００６４】（ｃ）基地局Ａからの登録受付情報を端末１が受信すると、今度は、端末１が、上記の図４に示した登録申請情報を基地局Ａへ送信する（ステップＳ４０４）。

【００６５】（ｄ）端末１からの登録申請情報を基地局Ａが受信すると、基地局Ａが、上記の図５に示した登録確認情報を端末１へ送信する（ステップＳ４０５）。この時、基地局Ａのモードは登録モードから認証モードに切り替わる。また、タイマ１が正常終了すると共に、タイマ２がスタートする。基地局Ａから送信される登録確認情報は、上記の第１の実施例で述べたように、登録申請した端末１の公開鍵で暗号化されているので、端末１だけがその内容を読むことができる。

【００６６】（ｅ）端末１は、基地局Ａからの登録確認情報を正しく復号できると、上記の図２０に示した認証申請情報を基地局Ａへ送信する（ステップＳ４０６）。この時、端末１のモードは、登録モードから認証モードに切り替わる。また、タイマ３が正常終了し、タイマ４がスタートする。図２０の認証申請情報は、端末１の秘密鍵を用いて暗号化されているので、この鍵と対を成している公開鍵を利用しないと復号できない。これは、端末１によるデジタル署名と考えることができる。この署名によって、認証申請情報が、上記の（ａ）乃至（ｄ）によって登録完了した端末１が送出したものであるか否かを判定することができる。

【００６７】（ｆ）基地局Ａは、端末１の公開鍵を知っているので、端末１からの認証申請情報を復号することができる。そして、基地局Ａは、上記の図６に示した認証通知情報を端末１へ送信する（ステップＳ４０７）。この認証通知情報は、端末１の公開鍵で暗号化されており、その鍵と対を成している秘密鍵によって復号される。

【００６８】（ｇ）この復号によって、基地局Ａの秘密鍵などを正しく取り出せると、上記の図７に示した認証受領情報を基地局Ａへ送信する（ステップＳ４０８）。この時、端末１は（登録済み）通常モードになり、タイマ４も正常終了する。

【００６９】（ｈ）端末１からの認証受領情報が基地局Ａで受理されると、基地局Ａも通常モードに戻り、タイマ２も正常終了する。ここで、端末１の登録・認証が完了する。

【００７０】以上説明したように、この第４の実施例は、上記の第１乃至第３の実施例と異なり、全体の処理が基地局Ａ主導であるという特徴がある。この第４の実施例によれば、端末１の登録ボタンを操作してから、端末１のタイマ３がタイムアウトする前に、基地局Ａの登

録ボタンを操作する必要がある。このため、家屋内にある基地局Ａを外部から操作することが困難なことと合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【００７１】（第５の実施例）次に、図２４および図２５を用いて、本発明の実施の形態に係る無線通信システムの第５の実施例を説明する。図２４は、この第５の実施例に係る無線通信システムの登録・認証シーケンスチャートである。図２４の登録・認証シーケンス（登録・認証シーケンス５）が上記の第４の実施例の登録・認証シーケンス４と異なる点は、時刻ｆで端末１が認証申請情報を基地局Ａへ送信する際、認証ボタンを利用することである。このようにすると、利用者が、端末１が登録モードから認証モードに切り替わったことを確認した後で、端末１の認証ボタンで認証申請することができる。上記の登録・認証シーケンス４と比べると、認証ボタンの分だけ手間が増すが、利用者に認証動作をより意識させる効果がある。

【００７２】図２５は、基地局Ａと端末１との間で交換される情報に焦点をあてて、図２４の登録・認証シーケンス５を説明するものである。図２５の丸囲み数字は登録・シーケンスの進行順を示すものである。この登録・認証シーケンス５では、端末１から基地局Ａへ登録申請情報、認証申請情報および認証受領情報が無線通信される。一方、基地局Ａから端末１へ登録受付情報、登録確認情報および認証通知情報が無線通信される。

【００７３】この第５の実施例によれば、端末１の登録ボタンを操作してから、端末１のタイマ１がタイムアウトする前に、基地局Ａの登録ボタンを操作する必要があり、また、端末１が認証モードに切り替わった後、基地局Ａのタイマ２がタイムアウトする前に、端末１の認証ボタンを操作する必要がある。このため、家屋内にある基地局Ａを外部から操作することが困難なことと合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【００７４】（第６の実施例）次に、図２６および図２７を用いて、本発明の実施の形態に係る無線通信システムの第６の実施例を説明する。図２６は、この第６の実施例に係る無線通信システムの登録・認証シーケンスチャートである。図２６の登録・認証シーケンス（登録・認証シーケンス６）が上記の第５の実施例の登録・認証シーケンス５と異なる点は、時刻ｆで端末１ではなく基地局Ａの方で、認証ボタンを利用する点である。この操作によって、基地局Ａが上記の図６に示した認証通知情報を端末１に送信する。登録・認証シーケンス５のように端末１が認証申請情報を送信する必要がない。つまり、端末１が登録モードから認証モードに切り替わったことを確認した後で、基地局Ａの認証ボタンを押すということが、認証申請情報の送信に取って代わっている。また、第４の実施例の登録・認証シーケンス４との比較では、認証ボタンの分だけ手間が増すが、利用者に認証動作をより意識させる効果がある。

【００７５】図２７は、基地局Ａと端末１との間で交換される情報に焦点をあてて、図２６の登録・認証シーケンス６を説明するものである。図２７の丸囲み数字は登録・シーケンスの進行順を示すものである。この登録・認証シーケンス６では、端末１から基地局Ａへ登録申請情報および認証受領情報が無線通信される。基地局Ａから端末１へ登録受付情報、登録確認情報および認証通知情報が無線通信される。

【００７６】この第６の実施例によれば、端末１の登録ボタンを操作してから、端末１のタイマ１がタイムアウトする前に、基地局Ａの登録ボタンを操作する必要があり、また、端末１が認証モードに切り替わった後、端末１のタイマ４がタイムアウトする前に、基地局Ａの認証ボタンを操作する必要がある。このため、家屋内にある基地局Ａを外部から操作することが困難なことと合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【００７７】（無線基地局）次に、本発明の実施の形態に係る無線通信システムに適用される無線基地局について説明する。図２８は、本発明の実施の形態に係る無線基地局のシステム構成を示すブロック図である。図２８に示すように、この基地局１０は、状態設定部１０１と、状態表示部１０２と、システム認証情報管理部１０３と、端末認証情報管理部１０４と、タイマ設定部１０５と、無線通信部１０６と、コントローラ１０７と、を備えている。

【００７８】状態設定部１０１は、登録モードや認証モードのボタンである。状態表示部１０２は、たとえば、上記の第１乃至第６の実施例で述べたＬＥＤ表示である。また、ＬＥＤ表示以外としては、液晶などの表示画面へのインストラクション表示、ＬＥＤの脇に印刷された文字列による指示、音声による指示、メロディによる表示、ネットワーク接続された他ノード画面へのインストラクション表示なども考えられる。

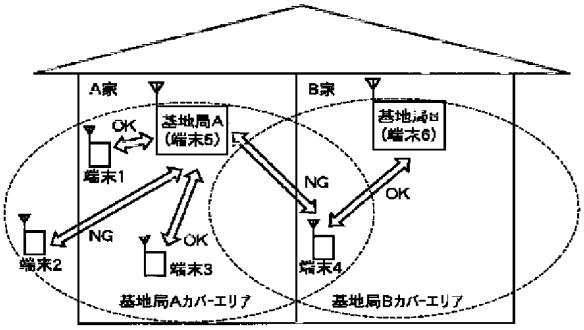
【００７９】システム認証情報管理部１０３は、この基地局１０の管轄システム内で使用される共通鍵暗号方式を管理する。共通鍵暗号方式の秘密鍵と暗号アルゴリズムとが管理されており、外部から容易には読み出せないようにしておく必要がある。端末認証情報管理部１０４では、この基地局１０が管轄するシステムにおいて登録・認証済みの端末について、端末固有情報と公開鍵と暗号アルゴリズムとが、上記の図９に示した登録認証テーブルに管理されている。なお、基地局１０自体の、端末としての、端末固有情報と公開鍵暗号方式の情報も管理されている。

【００８０】タイマ設定部１０５は、上記の第１乃至第６の実施例で登場した基地局１０のタイマを管理しており、そのスタートや終了を制御する。無線通信部１０６

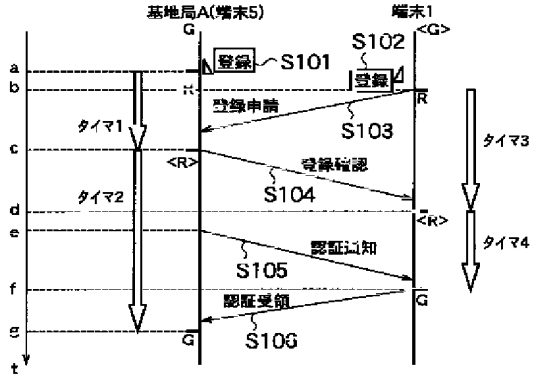
は、無線により端末と情報の交換を行う部分である。
【００８１】（無線端末）次に、本発明の実施の形態に係る無線通信システムに適用される無線端末について説明する。図２９は、本発明の実施の形態に係る無線端末のシステム構成を示すブロック図である。図２９に示すように、この端末２０は、状態設定部２０１と、状態表示部２０２と、システム認証情報管理部２０３と、端末情報管理部２０４と、タイマ設定部２０５と、無線通信部２０６と、コントローラ２０７と、を備えている。
【００８２】状態設定部２０１は、図２８の状態設定部１０１と同様、登録モードや認証モードのボタンである。状態表示部２０２は、図２８の状態表示部１０２と同様、たとえば、ＬＥＤ表示である。システム認証情報管理部２０３は、登録・認証を受けた基地局の管轄システム内の共通鍵暗号方式を保存する。共通鍵暗号方式の秘密鍵と暗号アルゴリズムとが管理されており、図２８のシステム認証情報管理部１０３と同様、外部から容易には読み出せないようにしておく必要がある。端末情報管理部２０４は、この端末２０の固有情報と公開鍵暗号方式の情報とを管理している。タイマ設定部２０５は、上述の実施例１～６で登場した端末２０のタイマを管理しており、そのスタートや終了を制御する。無線通信部２０６は、無線により基地局と情報の交換を行う部分である。
【００８３】さて、上記の第１乃至第６の実施例の登録・認証シーケンス１乃至６を用いれば、基地局が管理するシステムに端末を登録・認証することが可能であることを説明してきた。本発明のように、ボタンなどのマニュアル操作と、ＬＥＤなどによる状態表示と、公開鍵方式と、共通鍵方式とを組み合わせると、通常のデータ通信と同じ無線方式で登録・認証を行うことができ、成功したか失敗したか状態表示されるので利用者が容易に判断でき、また、外部から家屋内の基地局をマニュアル操作することは困難であるので、無線通信によりながらも、セキュアかつ容易な登録・認証が実施できる。
【００８４】また、家庭内無線システムでは、基地局を複数用意して、個人やグループや家族全員など任意の単位で、柔軟に設定できると望ましいと考えられるが、これにも対応可能である。たとえば、図３０のようなケースである。１軒の家（Ｘ家と呼ぶ）の中には、Ａ氏専用の基地局Ａと、Ｂ氏専用の基地局Ｂと、家族全員用の基地局Ｘとが設置されている。基地局Ａは、Ａ氏の端末３だけを登録・認証する。一方、基地局Ａエリア内の、屋外の通りすがりの端末２や、Ｂ氏用端末４の登録・認証は拒否する。同様にして、基地局Ｂには、Ｂ氏の端末４だけが登録・認証される。基地局Ｘは、Ｘ家にある全端末を登録・認証するものであって、端末３や端末４だけでなく、基地局Ａや基地局Ｂも端末として登録・認証する。なお、このような場合、端末の通常モードは１種類で、端末は複数の基地局に登録・認証することが可能となっている。また、このような場合、各端末には、複数基地局の共通鍵暗号方式の秘密鍵と暗号アルゴリズムが、システム認証情報蓄積部に管理されるようになる。たとえば、端末３には、基地局Ａと基地局Ｘの秘密鍵と暗号アルゴリズムが管理される。
【００８５】
【発明の効果】本発明によれば、家庭内無線通信システムにおいて確実かつ容易な登録・認証を実行できる無線端末、無線基地局、家庭内無線通信システム、および、登録・認証方式を実現できる。
【図面の簡単な説明】
【図１】本発明に係る無線通信システムを説明する図である。
【図２】本発明に係る登録・認証方法の第１の実施例を示すシーケンスチャートである。
【図３】基地局Ａと端末１との間で交換される情報に焦点をあてて、図２のシーケンスチャートを説明する図である。
【図４】登録申請情報の内容を説明する図である。
【図５】登録確認情報の内容を説明する図である。
【図６】認証通知情報の内容を説明する図である。
【図７】認証受領情報の内容を説明する図である。
【図８】本発明に係る無線通信システムにおける登録・認証後の端末間での通信データの内容を説明する図である。
【図９】基地局の登録認証テーブルの内容を説明する図である。
【図１０】図２のシーケンスチャートのタイマの動作を説明する図である（その１）。
【図１１】図２のシーケンスチャートのタイマの動作を説明する図である（その２）。
【図１２】図２のシーケンスチャートのタイマの動作を説明する図である（その３）。
【図１３】図２のシーケンスチャートのタイマの動作を説明する図である（その４）。
【図１４】図２のシーケンスチャートのタイマの動作を説明する図である（その５）。
【図１５】本発明に係る登録・認証方法の第１の実施例において登録・認証が１回につき１端末限定であることを説明する図である。
【図１６】本発明に係る登録・認証方法の第２の実施例を示すシーケンスチャートである。
【図１７】基地局Ａと端末１との間で交換される情報に焦点をあてて、図１６のシーケンスチャートを説明する図である。
【図１８】本発明に係る登録・認証方法の第３の実施例を示すシーケンスチャートである。
【図１９】基地局Ａと端末１との間で交換される情報に焦点をあてて、図１８のシーケンスチャートを説明する図である。

【図２０】認証申請情報の内容を説明する図である。
【図２１】本発明に係る登録・認証方法の第４の実施例を示すシーケンスチャートである。
【図２２】基地局Ａと端末１との間で交換される情報に焦点をあてて、図２１のシーケンスチャートを説明する図である。
【図２３】登録受付情報の内容を説明する図である。
【図２４】本発明に係る登録・認証方法の第５の実施例を示すシーケンスチャートである。
【図２５】基地局Ａと端末１との間で交換される情報に焦点をあてて、図２４のシーケンスチャートを説明する図である。
【図２６】本発明に係る登録・認証方法の第６の実施例を示すシーケンスチャートである。
【図２７】基地局Ａと端末１との間で交換される情報に焦点をあてて、図２６のシーケンスチャートを説明する図である。
【図２８】本発明に係る無線基地局の概略構成図である。
【図２９】本発明に係る無線端末の概略構成図である。
【図３０】本発明に係る他の無線通信システムを説明する図である。
【図３１】ＩＥＥＥ８０２．１１ＷＥＰアルゴリズムにおける暗号化アルゴリズムを示す図である。
【図３２】ＩＥＥＥ８０２．１１ＷＥＰアルゴリズムにおける通信データフレームを示す図である。
【図３３】ＩＥＥＥ８０２．１１ＷＥＰアルゴリズムにおける復号化アルゴリズムを示す図である。
【図３４】ＩＥＥＥ８０２．１１ＷＥＰアルゴリズムによる認証のシーケンスチャートである。
【符号の説明】
１０　無線基地局
２０　無線端末
１０１，２０１　状態設定部
１０２，２０２　状態表示部
１０３，２０３　システム認証情報管理部
１０４　端末認証情報管理部
１０５，２０５　タイマ設定部
１０６，２０６　無線通信部
１０７，２０７　コントローラ
２０４　端末情報管理部

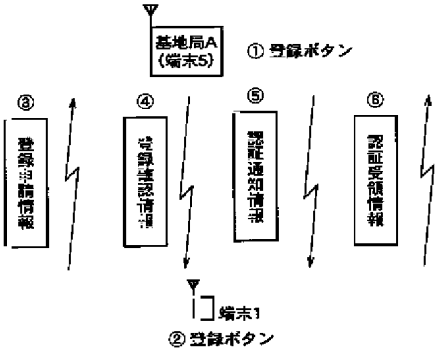
【図１】



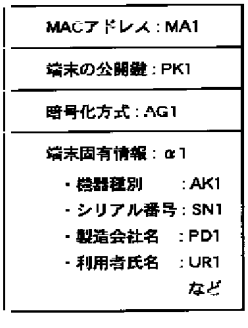
【図２】



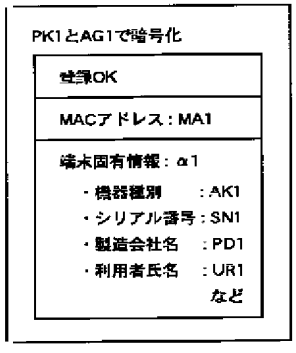
【図３】



【図４】

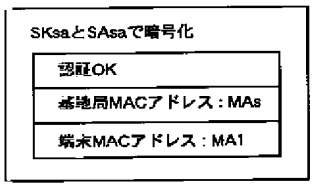


【図５】



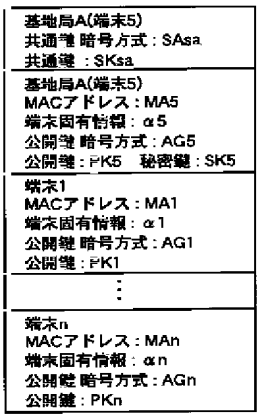
【図６】

【図7】

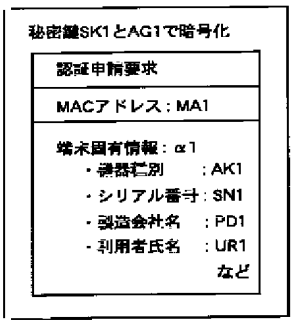


【図8】

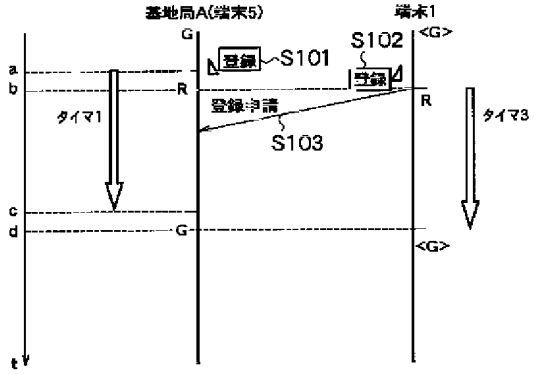
【図9】



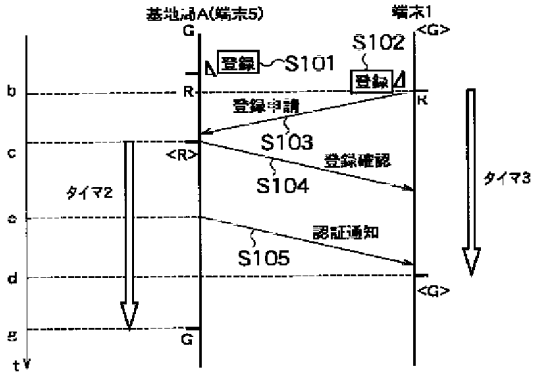
【図20】



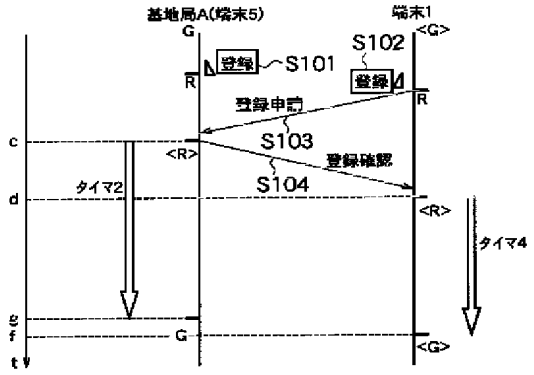
【図10】



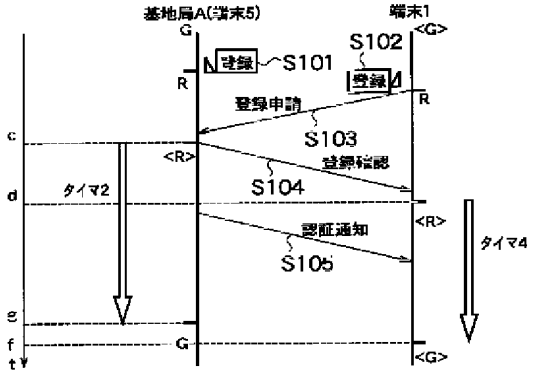
【図11】



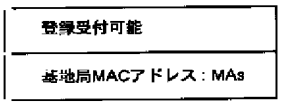
【図12】



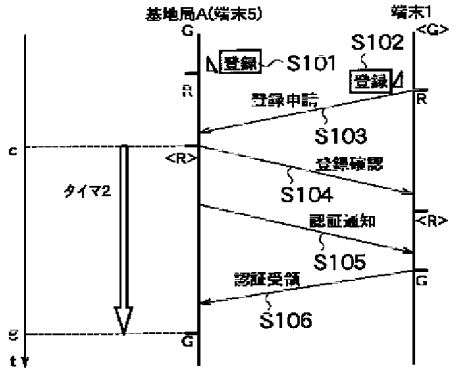
【図13】



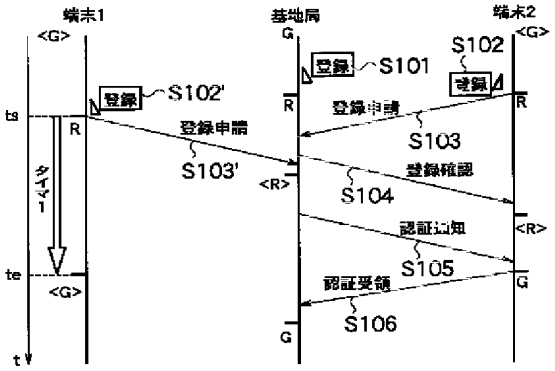
【図23】



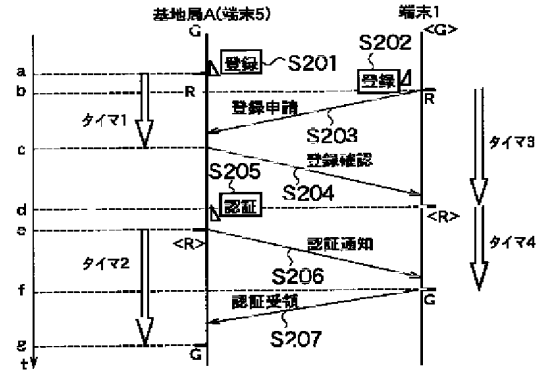
【図１４】



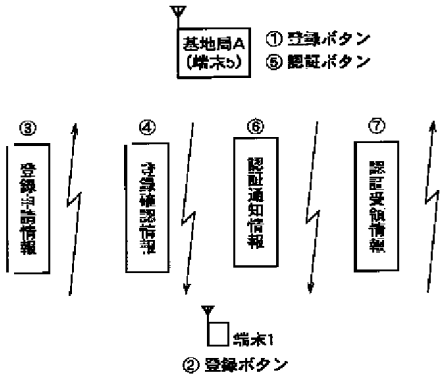
【図１５】



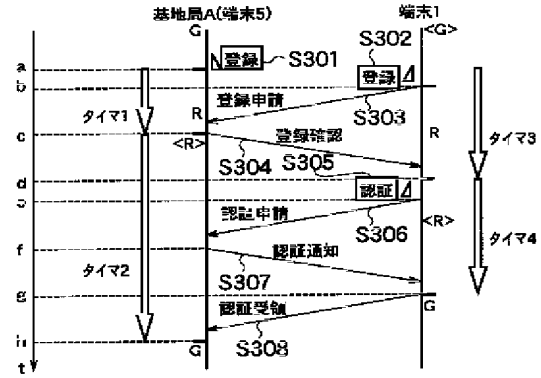
【図１６】



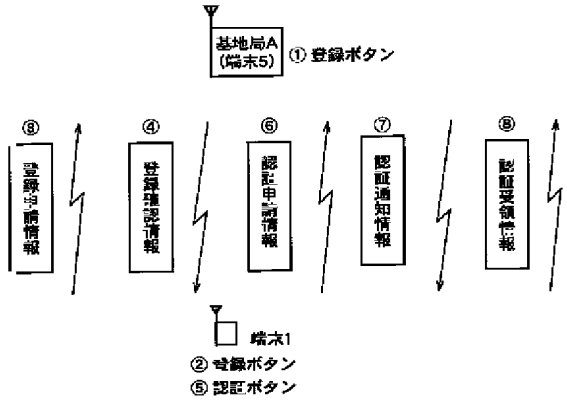
【図１７】



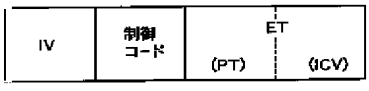
【図１８】



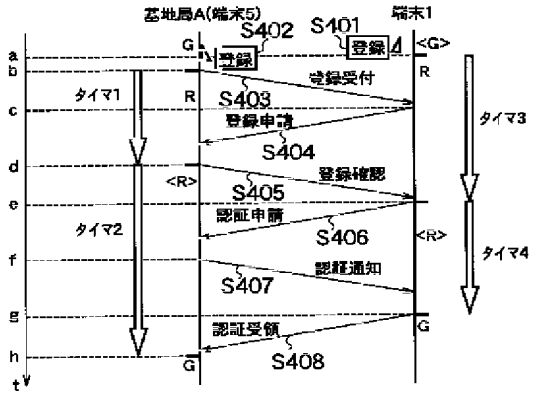
【図１９】



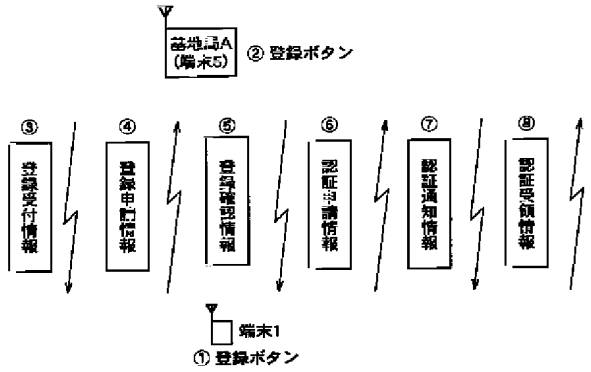
【図３２】



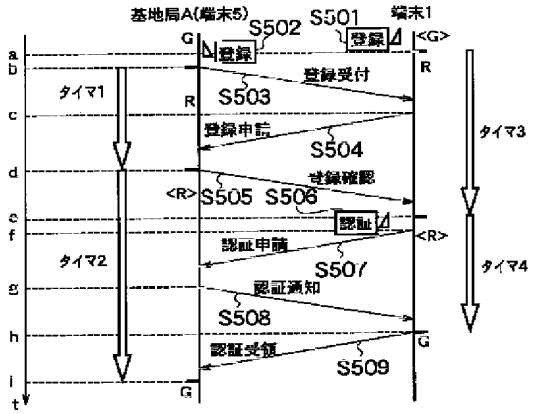
【図２１】



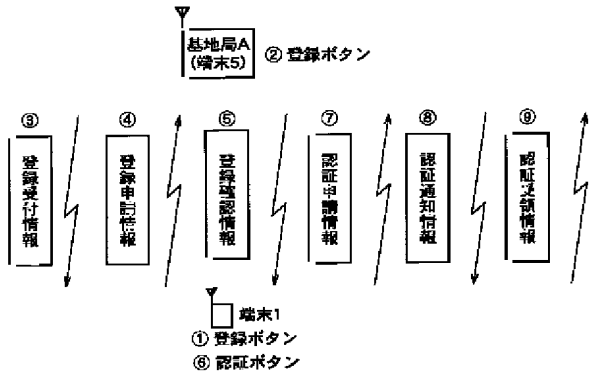
【図２２】



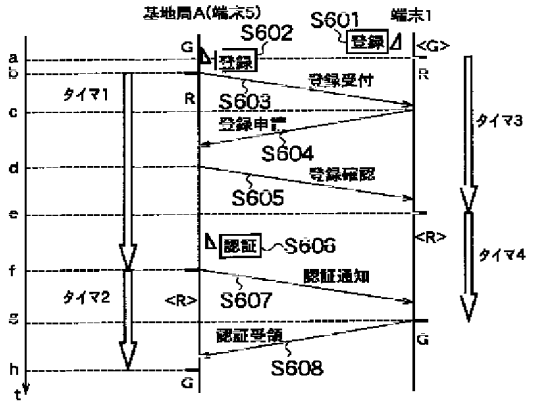
【図２４】



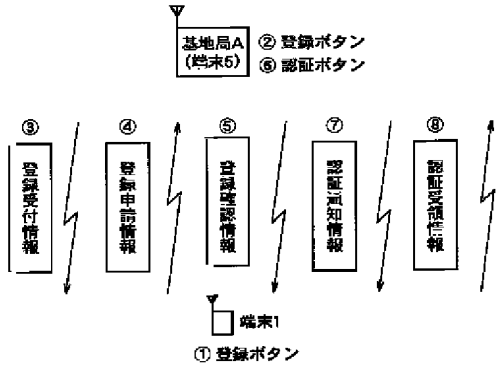
【図２５】



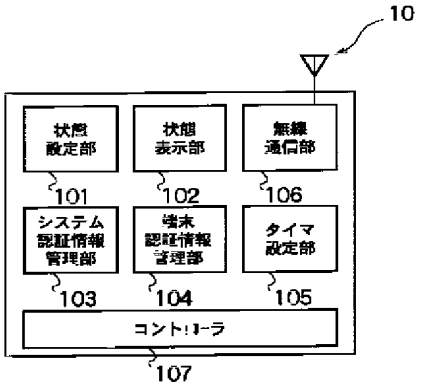
【図２６】



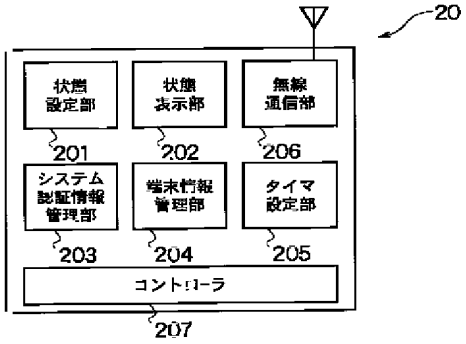
【図２７】



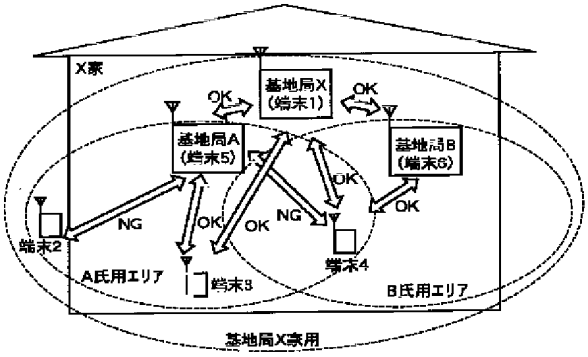
【図28】



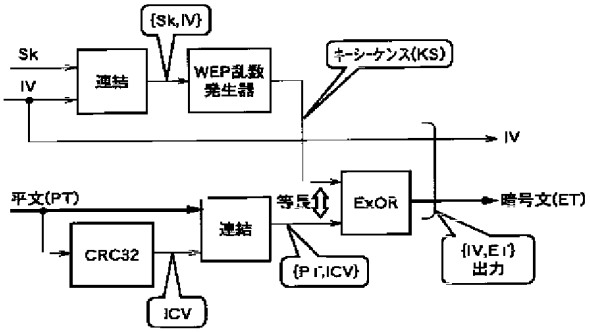
【図29】



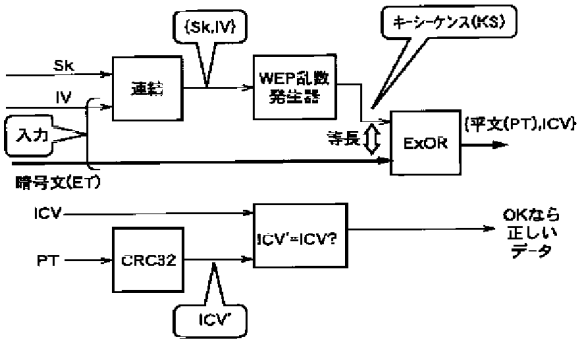
【図30】



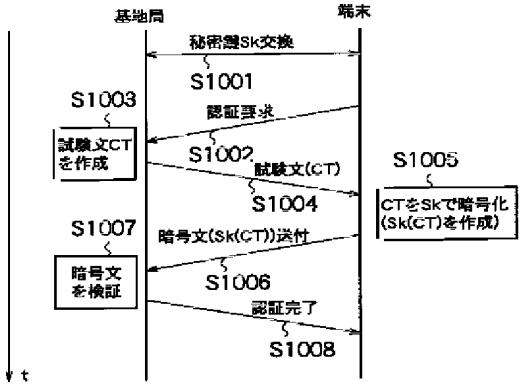
【図31】



【図32】



【図34】



フロントページの続き

Ｆターム(参考)　5J104 AA07 AA16 EA06 EA19 EA22
JA03 KA02 KA05 KA09 NA02
NA37 PA02
5K033 AA08 BA01 CC02 DA01 DA19
5K067 AA30 BB21 DD17 DD51 EE02
EE10 FF05 HH36